



Contivity® 1700, 2700 and 5000 Secure IP Services Gateways



FIPS 140-2 Non-Proprietary Security Policy

**Level 2 Validation
Version 1.8
December 2005**

Table of Contents

INTRODUCTION.....	3
PURPOSE	3
REFERENCES.....	3
DOCUMENT ORGANIZATION	3
CONTIVITY 1700, 2700 AND 5000.....	4
OVERVIEW	4
MODULE INTERFACES	4
ROLES AND SERVICES	5
<i>Crypto-Officer Role.....</i>	<i>5</i>
<i>User Role</i>	<i>6</i>
<i>Authentication Mechanisms.....</i>	<i>6</i>
PHYSICAL SECURITY.....	6
CRYPTOGRAPHIC KEY MANAGEMENT AND ALGORITHMS	6
<i>Critical Security Parameters of the Module</i>	<i>6</i>
<i>Key Generation</i>	<i>12</i>
<i>Key Storage.....</i>	<i>12</i>
<i>Key Protection/Zeroization</i>	<i>13</i>
SELF-TESTS	13
<i>Power-Up Self-Tests</i>	<i>13</i>
<i>Conditional Self-Tests</i>	<i>13</i>
DESIGN ASSURANCE	14
MITIGATION OF OTHER ATTACKS	14
SECURE OPERATION	15
INITIAL SET-UP	15
<i>Configuring the switch for FIPS operating mode</i>	<i>15</i>
CRYPTO OFFICER AND USER GUIDANCE	16
APPLYING TAMPER EVIDENCE LABELS	16
ACRONYMS	18

INTRODUCTION

Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Contivity 1700, 2700 and 5000 Secure IP Services Gateways from Nortel Networks with a firmware version of V04_85.121. This security policy describes how the Contivity 1700, 2700 and 5000 meet the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/cryptval/>.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Nortel Networks website (<http://www.nortel.com>) contains information on the full line of products from Nortel.
- The NIST Validated Modules website (<http://csrc.ncsl.nist.gov/cryptval/>) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Nortel Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Nortel Networks and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Nortel Networks. The Contivity 1700, 2700 and 5000 Secure IP Services Gateways will either be referenced as Contivity Modules, Contivity Gateways or Contivity Switches in this document.

CONTIVITY 1700, 2700 AND 5000

Overview

The Contivity 1700, 2700 and 5000 Secure IP Services Gateways are the ideal solution for enterprises requiring secure, low-cost connectivity across the Internet or managed IP networks. The Contivity 1700, 2700 and 5000 provide IP routing, Virtual Private Networking (VPN), stateful firewall, encryption, authentication, directory and policy services, Quality of Service (QoS), and bandwidth management services in a single integrated platform. The Contivity series scales across different user and throughput needs, with the Contivity 1700 being ideal for office centers, campuses, and large branch offices, the Contivity 2700 ideal for large organizations to extend secure remote access to many teleworkers and small offices, and the Contivity 5000 ideal for large organizations to extend secure access to thousands of teleworkers and remote sites.

The following are the version numbers of the network interface cards that can be used with the module.

Field Installable:

T3 HSSI WAN Interface - DM2111003
T1CSU/DSU WAN interface - DM2111005
Single V.35/X.21 WAN interface - DM2111006
Encryption accelerator - DM0011052
10/100 Ethernet - DM1011002

Factory Installable:

T3 HSSI WAN Interface - DM2104003
T1CSU/DSU WAN interface - DM2111004
Single V.35/X.21 WAN interface - DM2111007
Encryption accelerator - DM0011051
10/100 Ethernet - DM1004002

The Contivity modules support the HiFn 7811 chip, which is located on the encryption accelerators, for hardware cryptographic acceleration.

Module Interfaces

The Contivity 1700, 2700 and 5000 have been evaluated as multi-chip standalone modules, and the cryptographic boundary of the module is defined by the outer case of the module. The modules provide a number of physical and logical interfaces to the device.

The physical interfaces provided by the modules are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
-------------------	----------------------------

Data Input Interface	10/100BASE-TX LAN Ports, 10/100/1000 Ethernet port (only on 5000), WAN Port
Data Output Interface	10/100BASE-TX LAN Ports, 10/100/1000 Ethernet port (only on 5000), WAN Port
Control Input Interface	10/100BASE-TX LAN Ports, 10/100/1000 Ethernet port (only on 5000), WAN Port, Console Port, Power Button, Reset Button
Status Output Interface	LEDs, 10/100BASE-TX LAN Ports, 10/100/1000 Ethernet port (only on 5000), WAN Port, Console Port
Power Interface	AC 100 ~ 120 Vrms 6.2A Max.

Roles and Services

The modules support role-based authentication. The Crypto-Officer is authenticated using a username and password while the User can use a pre-shared key or a RSA digital signature to authenticate. The passwords conform to FIPS approved security requirements. The module can be accessed in two ways:

1. Through a command line interface (over a console port or over an IPSec tunnel in a FIPS mode of operation).
2. Through a Web-based interface (over a TLS session in a FIPS Mode of operation).

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and User role.

Crypto-Officer Role

The Crypto-Officer is the administrator of the Gateway and does the initial set up and maintenance. At the highest level, Crypto-Officer Services include the following:

- Configure the Gateway: define network interfaces and settings, set the protocols the gateway will support, define routing tables, set system date and time, and load authentication information.
- Create user groups: define common sets of user permissions, including access hours, call admission priority, forwarding priority, number of simultaneous logins, maximum password age, minimum password length, whether passwords contain only alphabetic characters, whether static IP addresses are assigned, idle timeout, forced logoff for timeout, protocols allowed, filters applied, and types of

encryption allowed. Administrators can define the permission sets for a number of users by creating, editing, and deleting user groups.

- Create users: define user accounts and assign them permissions using user groups. Additionally, an account can be assigned an administrator ID allowing access to the Crypto Officer role. Each administrator ID is assigned rights to manage the gateway (either *none*, *view switch*, or *manage switch*) and rights to manage Users (either *none*, *view users*, or *manage users*).
- Set up services: Initialize and configure services in the module - RADIUS, VPN, Firewall service, Circuit-less IP, backup interfaces and logging interface (syslog).
- Configure cryptographic keys and functionality: Install necessary identity key pairs and set the necessary pass-phrases (like the RADIUS shared secret).
- Define rules and filters: create packet filters that are applied to user data streams on each interface. Each filter consists of a set of rules, which define a set of packets to permit or deny basic characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction. The administrator can use any of the predefined rules or create custom rules to be included in each filter.
- Status functions: view the switch configuration, routing tables, and active sessions; and use Gets to view SNMP MIB II statistics, usage graphs, health, temperature, memory status, voltage, packet statistics, and review accounting logs.
- Manage the switch: log off users, shut down or reset the switch, disable or enable audible alarms, manually back up switch configurations, restore switch configurations, or create a recovery diskette.

User Role

The user is someone that sends data through the gateway. A user authenticates as necessary to initiate secure tunnels using the services (IPSec, PPTP, L2F and L2TP) of the module. Once authenticated, a user can access these services to send data through the module.

Authentication Mechanisms

The Contivity modules provide three ways of authentication. The document *Configuring the Contivity in FIPS Mode* makes recommendations and lists guidelines to run the switch in a secure FIPS approved mode.

Authentication Type	Strength
Password	The module supports password-based authentication for the Crypto-Officer through the password records stored on the module. The minimum size of the password can be chosen by the Crypto-Officer and the module supports password sizes of up to even 16 characters and passwords a minimum of 6 characters in length must be used in FIPS mode. Assuming only 36

	characters (A-Z, a-z, and 0-9) with repetition, the chance of a random attempt falsely succeeding is 1 in 56800235584.
RADIUS shared secret key	The RADIUS server authenticates to the module using a hash of the shared secret key combined with other information. The minimum size of this shared secret key configured by the Crypto-Officer must be 6 characters in length in FIPS mode. Assuming usage of only the 94 ASCII characters capable of being entered through a keyboard with repetition, the chance of a random attempt falsely succeeding is 1 in 689869781056.
Public Key based	The module supports authentication using RSA public keys for IPsec and TLS. The probability of a random attempt to falsely succeed is much lesser than 1 in 2^{512} .
Pre-shared keys	This method of authentication derives the pre-shared keys based on the user id and password using SHA-1. The probability of a random attempt to falsely succeed is much less than 1 in 2^{160} .

The module supports both an internal and external RADIUS server based authentication. The Crypto-Officer can either configure the authentication to be performed using data in an internal LDAP or RADIUS server, or using an external RADIUS or LDAP server. If the RADIUS server is used, only a CHAP based authentication must be used. In other words, PAP must be disabled.

Physical Security

The Contivity 1700, 2700 and 5000 are multi-chip standalone modules and meet all physical security requirements for FIPS 140-2. The platforms provide production grade equipment, industry-standard and a strong enclosure, and the systems meet Federal Communication Commission (FCC) Electromagnetic Interference (EMI) compatibility requirements. The document *Configuring the Contivity in FIPS Mode* defines the required procedures to apply tamper-evidence labels across the module's cover so that the Crypto-Officer can detect any attempt to open the box. It also details logging all access to the box by logging each time the tamper evidence seals are broken with permission of the Crypto-Officer. The module also has an audible alarm that activates when the front cover is removed.

Cryptographic Key Management and Algorithms

Critical Security Parameters of the Module

Only the Crypto-Officer (Administrator) can log on to the box directly through the console or the web interface. Normal users of the box only access it through the services. So the CSPs are accessed directly only by the Crypto-Officer. All other users access them through protocol.

The following Critical Security Parameters are used in the module:

Cryptographic Key	Description	Key Type	Storage and Zeroization
User and Crypto-officer Passwords	These passwords are used in PAP, CHAP, PPTP, L2TP, L2TF and in generating IPsec pre-shared keys.	An alpha-numeric string with a minimum length of 6 characters.	The passwords of the user and Crypto-Officer are stored in the LDAP database. They are zeroized by overwriting them with new passwords when the user or Crypto-Officer changes the password.
DES key used for Integrity check and software/firmware load test for Software upgrades	This key is used to perform the integrity check on the module. The key is also used to perform software/firmware load test for software upgrades.	A DES key of 56 bit length	This key is compiled into the Contivity device code and can be zeroized using the "Reformat Diskette" button on the Web interface. In order to zeroize this key, the Crypto-Officer must click the "Reformat Diskette" button on the Web interface. The format utility then causes the firmware to be erased, effectively zeroizing the key.
IPsec User pre-shared keys	These are derived from the user name and password. It is the responsibility of the Crypto-Officer to configure the username and password to match on both ends of the connection. These pre-shared keys are used in the IPsec User tunnels.		These are generated and stored in the LDAP database if the Crypto-Officer configures to use the pre-shared keys for the particular user. These are zeroized when the module is reset or when the user passwords are changed.

IPSec Branch Office pre-shared keys	These pre-shared keys are used in the IPSec Branch Office tunnels. The key is entered via the console port or the Web interface.		These are stored in the LDAP database and are zeroized when the module is reset or when a new value is entered.
IPSec Session Keys	These are exchanged using IKE protocol and the public-private key pairs.	The type and size of the session keys depend on the algorithm used. So it is an AES, 3DES or DES key.	They are not stored on disk. They are stored in the RAM memory during the session and are zeroized when the session ends.
IPSec HMAC SHA-1 keys	These are used to check for message integrity during IPSec data exchange.	These are HMAC SHA-1 keys.	These are ephemeral keys not stored on disk. These are stored in RAM and are zeroized when the session ends.
TLS Session Keys	These are exchanged during the tunnel establishment using the public-private key pairs of either end of the tunnel.	The type and size of the session keys depend on the algorithm used. So it is either an AES, 3DES or DES key.	They are not stored on disk. They are stored in the RAM memory during the session and are zeroized when the session ends.
X.509 certificates	These include the module's public key and also the certificates of other hosts and users accessing the system. They are used in IPSec key negotiation using Diffie-Hellman and TLS key negotiation.	RSA public key based certificates	They are stored in files in the module. Every certificate is stored in a separate file.
Private Key	This is the module's private key for Diffie-Hellman key exchange for IPSEC and TLS key negotiation	RSA private key	The private key is stored encrypted using a PKCS#5 password based encryption. The password itself is not stored but a MAC of the plaintext private key is stored to verify the password. The encryption is not FIPS approved and so for FIPS purposes it is stored in plaintext. These are zeroized when

			the Crypto-Officer clicks the “Delete” button associated with these keys on the Web interface.
RADIUS Shared Secret	Entered by the Crypto-Officer in form through the web interface over a TLS session and stored in plain-text form.	Pass-phrase. Alphanumeric string.	The shared secret is stored in the internal LDAP database in plaintext form (PKCS#5 encrypted but considered plaintext for FIPS purposes). It is zeroized, by overwriting the secret key with a new value through the web interface over a TLS session.

The module has a configurable password mechanism where the Crypto-Officer can set a maximum password length of 16 characters. It is required that the minimum length be 6. The CSPs are accessible only to the Crypto-Officer. The users can only change their passwords but cannot view/access the keys of other users on the module. The module encrypts (PKCS#5) all the passwords and CSPs stored in the LDAP database using a string derived from a pass-phrase, but for FIPS purposes they are stored in plaintext form. The pass-phrase is stored hard-coded in the software.

IKE

The Switch performs Internet Key Exchange (IKE) (ISAKMP-Oakley) in both main-mode and aggressive mode key exchanges. These are protocols based on Diffie-Hellman key exchanges. IPsec explicitly negotiates a common key during the ISAKMP exchange, and also refreshes it periodically. The switch can also use the pre-shared key option of IPsec for aggressive mode for authentication purposes. Key generation is done per ISAKMP-Oakley.

TLS

The switch also performs server-side authentication using TLS to perform key exchange. Server certificates are stored on the device and used to generate ephemeral session keys. Access to an external LDAP server must be through a TLS connection.

Algorithms

The switch supports the following cryptographic algorithms.

The Contivity switches support the following Approved cryptographic algorithms:

Symmetric Key Algorithms:

Algorithm	Modes Implemented	Key Sizes
AES (FIPS 197)	CBC	128 Bits
DES (FIPS 46-3)	CBC	56Bits (to be used for legacy systems only), 40Bits (may not be used in FIPS mode)
3DES (FIPS 46-3)	CBC	112,168 Bits

Hashing Algorithms:

Algorithm
SHA-1 (FIPS 180-1)

Message Authentication Algorithms:

Algorithm
DES-MAC (FIPS 113)
HMAC SHA-1 (FIPS 198)

Public Key Algorithms:

Algorithm	Key Sizes
RSA (PKCS#1)	1024, 2048 Bits; 512, 768 Bits (may not be used in FIPS mode)

The modules contain both hardware and software algorithm implementations of the following algorithms: DES, 3DES, SHA-1 and HMAC SHA-1.

The certificate numbers for the algorithms are given below:

Algorithm	Software Implementation	Hardware Implementation
DES	48	101
3DES	183	29
AES	50	Not implemented
SHA-1	31	51

Additionally, the module is permitted to use the following non-FIPS Approved algorithms in a FIPS mode of operation:

Key Exchange Algorithm:

Algorithm
Diffie-Hellman

The module also includes the following non-FIPS Approved algorithms:

Symmetric Key Algorithms:

Algorithm	Key Sizes
RC2	128 Bits
RC4	40Bits, 128Bits
DES	40 Bits

Hashing Algorithms:

Algorithm
MD5
MD2

Message Authentication Algorithms:

Algorithm
HMAC MD5

Password-Based Encryption:

Algorithm
RSA (PKCS#5)

Key Generation

The module implements the FIPS 186-2 based PRNG. All key generation functions use the approved PRNG implementation. The module generates private-public key pairs. It also uses the PRNG implementation to generate keys for IPsec and TLS negotiations.

Key Storage

The module stores keys internally. The keys are shielded from outside access and only Crypto-Officers can access them. The private keys are stored encrypted with a password based string based on PKCS#5 specification. User passwords are stored in the switch in an encrypted form in the internal LDAP database. A fixed key/pass-phrase string (which is compiled into the module code) is used to encrypt the passwords. For FIPS purposes,

these keys are considered to be in plaintext form. The access rights set on each of the CSPs do not matter because only the Crypto-Officer has direct access to them.

Key Protection/Zeroization

Only the Crypto-Officer can access the keys. The module has a password-based authentication mechanism for the administrator. Also the interface through which the administrator logs in is different from the user interface for additional security.

The switch securely administers both cryptographic keys and other critical security parameters, such as operator passwords. Ephemeral session keys are created during the negotiation of secure tunnels on behalf of users who have successfully authenticated themselves to the switch with their user ID and password. These keys are created for protocols like MS-CHAP and ISAKMP, which securely negotiate key exchange and then allow encryption services for PPTP, L2TP, and IPsec. Keys are destroyed when the appropriate tunnel, security association (SA), or session is terminated, and are never archived or released from the device. Private keys are always overwritten by new keys if need to be changed. User passwords can be destroyed by Crypto Officers or by users overwriting their own passwords. All passwords are stored in the LDAP database in an encrypted format and are never released. They are used only for authentication in key exchange protocols. Crypto Officers should be aware that Password Authentication Protocol (PAP) transmits password information in the clear and must not be enabled before deciding local policy. See *Configuring the Contivity VPN Switch* for more information on PAP.

Self-Tests

The module performs power-up and conditional self-tests to ensure the secure and proper operation, and the sections below provide details on the module's self-tests.

Power-Up Self-Tests

The power-up self-tests implemented by the module are a software/firmware integrity check, and known answer tests for AES, DES, 3DES, SHA-1, HMAC SHA-1, RSA and the PRNG. Power-up self-tests are executed automatically when the module is started.

Conditional Self-Tests

The module performs three conditional self-tests: a pair-wise consistency test each time a module generates RSA public/private key, a continuous random number generator test each time the module produces random data, and a software load test for upgrades.

If any of the self tests fail, the module enters an error state, logs the error to a file, and forcibly crashes the machine in a controlled manner.

Design Assurance

Nortel Networks follows highly stabilized and popular design procedures for both Software and Hardware implementations. The design for the Contivity follows FIPS provided guidelines. The software and hardware design both go through many phases of review and inspections. The code and design documents are securely stored and the delivery is also secure.

Mitigation of Other Attacks

The module does not claim to mitigate any attacks in the FIPS mode of operation.

SECURE OPERATION

This section describes the steps required to run the switch in a FIPS approved mode of operation. It also suggests standard security principles to ensure a more secure operation.

Initial Set-Up

Configuring the switch for FIPS operating mode

A number of protocols and features of the switch are not part of the permitted functions in a FIPS-compliant system.

The web-based management interface provides a button to enable FIPS mode. Place the module in FIPS mode by clicking on the FIPS Enabled button on the Services...Available management screen, and restart the module. Enabling FIPS mode disables these protocols and features.

The following are performed by the system after pushing the button to enable FIPS mode:

- The external LDAP server is disabled in FIPS mode. The module may still be configured to use an *internal* LDAP server or an internal/external RADIUS server.
- FTP is disabled in FIPS mode.
- Debugging scripts are disabled in FIPS mode.
- Change the default administrator password on the switch.
- Debugging scripts are disabled.
- The administrator is given additional authority to reset the default administrator's password and username.
- The 'NULL' encryption option is disabled for the IPsec services in FIPS mode. This ensures that the module is not in a bypass mode in a FIPS mode of operation.
- The system must be rebooted after enabling or disabling mode.

These additional actions must be performed by the Crypto-Officer to put the module in a FIPS mode.

- The default administrator password must be changed.
- Crypto-Officer passwords must be configured to be a minimum length of at least 6 characters.
- RADIUS shared secret keys must be set to be at least 6 characters long.
- LDAP proxying must be over a TLS session.
- Maximum number of login attempts must be configured to five (5)
- Tamper-evident labels must be applied per the Applying Tamper Evidence Labels section.
- All cryptographic services (PPTP, L2TP, L2F) that employ non-FIPS approved algorithms must be disabled. This includes SSL and all services using SSL.
- All access to the web based management interface must be over a TLS session.
- All network-based access to command line interface must be over an IPsec tunnel.

Additionally, the module has an audible alarm that is triggered if the front cover is removed. This can be enabled through the command line interface by the command “audible alarm” and disabled by the command “no audible alarm”.

Crypto Officer and User Guidance section contains instructions for Crypto Officer and Users to maintain the FIPS mode of operation. More details on FIPS mode configuration of the module can be found in the document “Using Contivity Secure IP Services Gateways in FIPS Mode.”

Crypto Officer and User Guidance

The document *Configuring the Contivity for FIPS Mode* gives a detailed list of actions that must be run to place the module in FIPS mode and also outlines the steps needed to perform them. This document is the Crypto Officer Guidance document. There is no specific User Guidance, as the configuration and management of the module are services of the Crypto Officer; thus, the User documentation for the module is sufficient User Guidance.

Applying Tamper Evidence Labels

Once the Contivity module has been configured in the FIPS 140-2 level 2 mode, the cover may not be removed without signs of tampering.

To seal the system on the 1700, 2700 or 5000, you must apply serialized, tamper-evident labels as follows:

1. Ensure that the temperature of the switch is above 10°C (Nortel Networks recommends a temperature of approximately 20°C).
2. Turn off and unplug the system.
3. Clean the chassis of any grease, dirt, or oil. The supplied alcohol-based cleaning pads are recommended for this purpose.
4. Apply labels as shown in Figure 1 (1700 and 2700) or Figure 2 (5000).
5. Record the serial numbers of the labels applied to the Contivity switch in a security log.
6. Allow *72 hours* for the adhesive in the tamper-evident seals to completely cure.

The following are diagrams illustrating where the tamper evidence labels are applied.

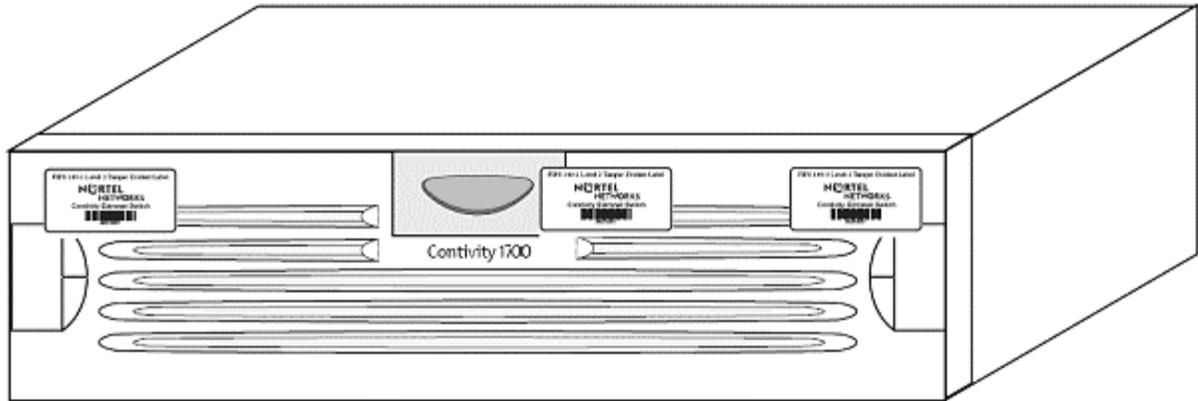


Figure 1 - Tamper evidence label for 1700 and 2700

To seal the 1700 and 2700 VPN routers, three tamper-evident labels need to be placed on the front bezel. Couple of the labels should be put on both the bezel screws and another should be overlapped on center section and bezel.

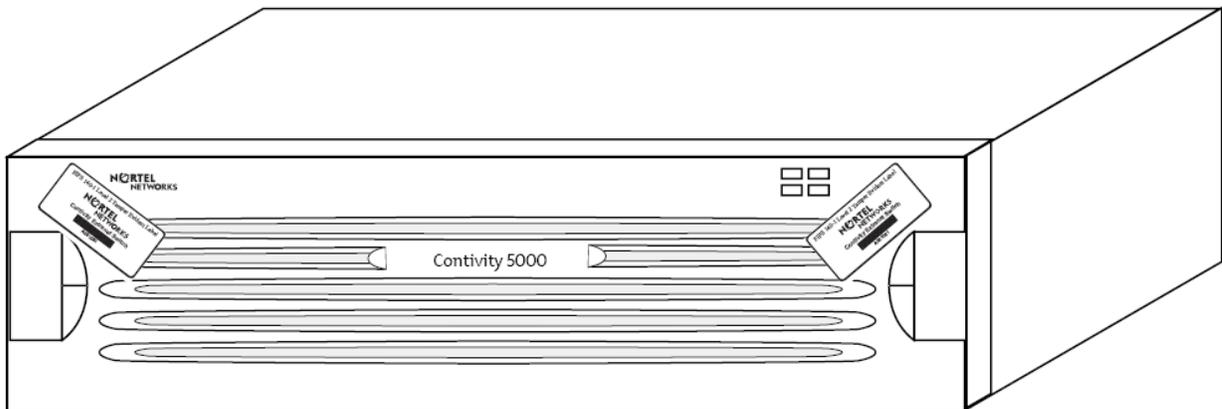


Figure 2 - Tamper evidence label for 5000

5000 router requires two tamper-evident labels on both the bezel screws to seal the module. For 5000 VPN router, labels should be placed in an angle to avoid molding the labels over the curved handles and also hide LEDs at front.

ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security